IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORIGA
ATLANTA DIVISION

Naomi Gordon, on behalf of her minor child N.L. individually and all others similarly situated, Plaintiff, v. NextGen Healthcare, Inc. Defendant.	)	**Case No.** **COMPLAINT – CLASS ACTION** **Jury Trial Demanded**

Plaintiff Naomi Gordon, on behalf of her minor child, N.L. ("Plaintiff") and all others similarly situated ("Class Members"), by and through her attorneys of record, upon personal knowledge as to Plaintiff's own acts and experiences, and upon information and belief as to all other matters, files this complaint against NextGen Healthcare, Inc., ("NextGen" or "Defendant") and alleges the following:

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons impacted by Defendant's failure to safeguard, monitor, maintain and protect highly sensitive Personally Identifiable Information ("PII"). Defendant collected, stored, and maintained N.L.'s and the Class's Sensitive Information as part of its ordinary business activities as a health record and practice management service provider.

2. On March 30, 2023, NextGen learned that its networks containing its customers' patients' PII were impacted during a cyberattack ("Data Breach").[1] Specifically, from March 29, 2023 to April 14, 2023, hackers had access to NextGen's computer and file systems, allowing the hackers access to individuals' PII. Defendant disclosed that its Data Breach exposed PII including N.L.'s and the Class Members' names, dates of birth, addresses, and social security numbers.

3. Although Defendant discovered the Data Breach on March 30, 2023, it inexplicably waited until April 28, 2023, to notify the individuals whose information was impacted by the Data Breach. The Data Breach notice admitted that Defendant's networks and systems had been breached and that the cyberattack exposed highly sensitive information.

4. The Data Breach impacted the sensitive personal information of approximately 1,049,375 individuals.

5. The type of information impacted by the Data Breach can be used to orchestrate a host of fraudulent activities, including financial fraud and identity theft. Indeed, the entire purpose of these types of data breaches is to obtain and misuse victims' PII or to sell it to fraudsters on the dark web. Consequently, all impacted

[1] A sample Notice of the Data Breach that Defendant sent to Plaintiff and Class Members is available at https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8/6102f57f-d60d-4b59-aa4d-7c30e68a2f68/document.html.

individuals are at a heightened and significant risk that their information will be disclosed to criminals and misused for attempted or actual fraud or identity theft.

6. As a result of Defendant's lax data security concerning its systems and servers, hundreds of thousands of Defendant's customers' patients have had sensitive details of their lives and identities accessed, viewed and stolen by malicious cybercriminals. These patients have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

7. Defendant's conduct, consequently, required Plaintiff and the Class to have to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their PII, including by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records. Minors such as N.L., additionally, may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done.

8. As such, Plaintiff and the Class bring this action to recover for the harm they suffered, and assert the following claims: negligence, negligence per se, and breach of implied contract.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant NextGen, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

10. This Court has general personal jurisdiction over Defendant NextGen because NextGen maintains its principal place of business in Atlanta, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because NextGen's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

12. **Plaintiff** Naomi Gordon and her minor child, N.L., are residents and citizens of Duluth, Minnesota. Defendant obtained and maintained the PII of Plaintiff's minor child and owed her a legal duty and obligation to protect and secure that PII from unauthorized access or disclosure.

13. Plaintiff received notice from NextGen via letter dated April 28, 2023, that her child was a victim of the Data Breach.

14. **Defendant** NextGen Healthcare, Inc. is a Georgia corporation with its principal place of business at 3525 Piedmont Road Northeast, Building 6, Suite 700, Atlanta, GA 30305.

FACTUAL BACKGROUND

A. Defendant Collected, Maintained and Stored Sensitive Information.

15. NextGen Healthcare, Inc. provides electronic health records and practice management services to doctors and other medical professionals.

16. Defendant is an experienced and sizeable company and boasts of having 48 years in the market, with 2,800 NextGen employees servicing one hundred thousand providers and one million connected caregivers.[2]

17. As an ordinary and regular part of the services that it provides to medical professionals, Defendant maintains personal patient information on behalf of those medical professionals. Defendant's Notice of Data Breach to its customers' patients admits that "[i]n support of the services we provide to your medical professionals, we maintain certain of your personal information on their behalf."[3]

18. The personal and medical information that Defendant maintains is highly sensitive. To obtain healthcare services, patients, like Plaintiff's minor child and the Class, must provide their medical providers with highly sensitive

[2] https://www.nextgen.com/company/about-us

[3] *See* Notice of Data Breach.

information, including PII. As a massive health records service provider, Defendant has aggregated PII obtained via its customers—who are medical institutions that collect and maintain (and consequently, provide to Defendant) a massive repository of data. That massive repository acts as a particularly lucrative, and foreseeable, target for data thieves looking to obtain and misuse or sell patient data.

19. Plaintiff and the Class had a reasonable expectation that Defendant would protect the PII that it collected and maintained, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect their information could cause substantial harm.

20. Defendant's Privacy Policy acknowledges the sensitivity of the information that it maintains, along with the legal requirements for Defendant to confidentially maintain such information. In particular, Defendant's Privacy Policy notes that it maintains "Personal Health Information as that term is defined in the Health Insurance Portability and Accountability Act of 1996 … and in regulations promulgated there under and [the information] may also be subject to regulation under state law."[4]

21. NextGen's Privacy Policy promises that it provides "products and services in a manner that complies with all applicable laws and regulations we are

[4] https://www.nextgen.com/legal/privacy-policy

aware of and/or become known to us and will continue to do so." The Privacy Policy further promises that "Personally identifiable patient … information shall remain confidential and shall not be released."[5]

22. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's minor child's and the Class's PII prior to, during, or after the Data Breach, but rather enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

B. Defendant Suffered a Massive Data Breach Exposing Patients' Sensitive Information.

23. On March 30, 2023, NextGen discovered that there was suspicious activity on its systems. NextGen claims to have initiated an investigation and taken containment measures at that point, but those measures were clearly insufficient. NextGen later admitted that the scope and duration of the Data Breach was such that third-party hackers had gained access to its systems from March 29, 2023, to April 14, 2023. Upon information and belief, during the Data Breach the hackers copied and exfiltrated substantial amounts of Plaintiff's minor child's and the Class's PII.

[5] *Id.*

24. Defendant eventually notified Class Members of the Data Breach, stating that there was "a security incident involving certain of your personal information," which NextGen was on notice of by "March 30, 2023, [when] we were alerted to suspicious activity on our NextGen Office system." NextGen further confirmed that the "personal information impacted by the incident included your name, date of birth, address, and social security number."[6]

25. The Notice of Data Breach recommended Plaintiff and her minor child and the Class take several time-consuming steps to mitigate the risk of harm from the Data Breach. Specifically, it recommends that the Data Breach victims "remain vigilant by reviewing your account statements and credit reports closely," and to report suspicious activity.[7]

26. NextGen did not provide this notice to the individuals whose information was exposed until April 28, 2023, despite learning its network was accessed by an unauthorized third party on March 30, 2023. Had Defendant provided notice sooner, Class members would have been able to take mitigatory steps sooner.

27. Given that Defendant was storing the PII of Plaintiff's minor child and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent

[6] Notice of Data Breach.
[7] *See* Notice of Data Breach.

and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at numerous healthcare institutions and a recent ransomware attack on Defendant put Defendant on notice that the higher personal data they stored might be targeted by cybercriminals.

28. Despite the highly sensitive nature of the information Defendant obtained, maintained, and stored, Defendant's recent ransomware attack, and the prevalence of health care data breaches, Defendant inexplicably failed to take appropriate steps to safeguard the PII of N.L. and the Class from being compromised. The Data Breach itself, and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the PII it oversaw.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm.

29. The personal, health, and financial information of Plaintiff's minor child and the Class is valuable and has become a highly desirable commodity to data thieves.

30. Defendant's failure to reasonably safeguard N.L.'s and the Class's PII has created a serious risk to N.L. and the Class, including both a short-term and long-term risk of identity theft.

31. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

32. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[8]

33. Stolen PII, including social security numbers, is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other

[8] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

34. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, fraudsters can steal and use a minor's information until the minor turns eighteen years old before the minor even realizes he or she has been the victim of an identity theft crime.[9]

35. The risk to minor Class members is substantial given their age and lack of established credit. The information can be used to create a "clean slate identity," and use that identity for obtaining government benefits, fraudulent tax refunds, and other scams. There is evidence that children are 51% more likely to be victims of identity theft than adults.[10]

36. Purchasers of PII use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional PII from the victim, as well as PII from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harm.

---

[9] Brett Singer, *What is Child Identity Theft?*, Parents (last visited Jan. 17, 2022), https://www.parents.com/kids/safety/tips/what-is-child-dentity-theft/.

[10] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 18, 2022), https://axioncyber.com/data-breach/how-data-breaches-affect-children/.

37. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

38. Defendant did not rapidly, or even reasonably, report to Plaintiff's minor child and the Class that their PII had been exposed or stolen. Instead, Defendant waited over four weeks after identifying the Data Breach before notifying the Class of the breach.

39. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[11]

40. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

[11] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[12]

41. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

42. The FTC cautions businesses that failure to protect PII and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.[13] Indeed, the FTC treats

[12] *Start With Security, A Guide for Business*, FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

[13] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

43. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[14] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[15] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[16]

44. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[17]

---

[14] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[15] *Id.*

[16] *Id.*

[17] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020),

45. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[18] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[19]

46. The need for sufficiently robust cybersecurity, and the attractiveness of its data to third parties, was well known by Defendant. NextGen experienced a ransomware attack just months prior to this Data Breach.[20]

47. As a healthcare data service engaged with numerous medical facilities servicing hundreds of thousands of patients, if not more, Defendant knew or should have known the importance of protecting the PII entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its

---

https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

[18] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[19] *Five worthy reads: The never-ending love story between cyberattacks and healthcare*, ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

[20] Andrea Fox, *NextGen Healthcare hit by BlackCat Ransomware*, HEALTHCARE IT NEWS (Jan. 24, 2023), https://www.healthcareitnews.com/news/nextgen-healthcare-hit-blackcat-ransomware.

systems were breached. These consequences include substantial costs to Plaintiff's minor child and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. N.L.'s and the Class's Sensitive Information is Valuable.

48. Unlike financial information, such as credit card and bank account numbers, the PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[21]

49. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[22] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number

[21] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

[22] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

sells for as much as $300 per number.[23] Those numbers are often then used for fraudulent tax returns.[24]

50. Consumers place a considerable value on their PII and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their PII, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[25] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

51. Defendant's Data Breach exposed a variety of PII, including dates of birth and Social Security numbers.

52. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[26] If the identity thief

[23] *Id.*

[24] *Id.*

[25] 11-Horn Hann, Kai-Lung Hui, *et al, The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[26] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

53. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

54. Cybercriminals recognize and exploit the value of PII. The value of PII is the foundation to the cyberhacker business model. Because the PII exposed in the Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff's minor child and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their PII.

F. Plaintiff's and N.L.'s Experiences

55. Plaintiff brings this action on behalf of her minor child, N.L., who received a notice from Defendant that her information was accessed without authorization during the Data Breach.

56. As a condition of receiving healthcare-related services, Plaintiff and N.L. provided medical providers with her highly personal information, including PII. In turn, N.L.'s medical providers retained NextGen, which maintained access to

and control over N.L.'s PII. Plaintiff and N.L. expected that this highly personal information would remain between them and N.L.'s medical providers.

57. However, on April 28, 2023, Plaintiff received notice from Defendant, which informed her of the Data Breach, that N.L.'s information had been impacted by the Data Breach, and that she faced a substantial and significant risk of her PII being misused. As noted above, as a minor, N.L. remains at heightened risk of identity theft and fraud because her credit, like other minors, is often unmonitored or monitored to a far less degree than an adult's credit and accounts.

58. Subsequent to and as a direct and proximate result of the Data Breach, N.L. experienced a substantial number of spam messages and phone calls, which Plaintiff and N.L. believe is related to N.L.'s information being placed in the hands of an illicit actor.

59. Plaintiff and N.L. are very careful about sharing and protecting sensitive PII. Plaintiff and N.L. have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured channel. Furthermore, Plaintiff and N.L. diligently choose unique usernames and passwords for her various online accounts. Finally, N.L. has never previously had her identity stolen, received a notice related to a Data Breach, or, to her knowledge, been impacted by a Data Breach.

60. Plaintiff and N.L. suffered actual injury from haver her sensitive informaiton exposed and/or stolen as a result of the Data Breach, including but not

limited to: (a) mitigation efforts, including educating and monitoring N.L.'s accounts and other efforts to monitor N.L.'s credit to ensure that her information is not being used for identity theft or fraud; (b) damages to and diminution of the value of her PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of her privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of mitigation efforts as a result of the data breach.

61. In addition, knowing that hackers accessed and/or stole N.L.'s PII and that this will likely be used in the future for identity theft, fraud, and related purposes has caused Plaintiff and N.L. to experience significant frustration, anxiety, worry, stress, and fear.

CLASS ALLEGATIONS

62. Plaintiff brings this action against NextGen on behalf of her minor child and all other persons similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

63. Plaintiff proposes the following Class definition:

> All persons who received notice that their information was or was potentially impacted by Defendant's Data Breach.

64. Excluded from the Class is Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in,

is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

65. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

66. All members of the proposed Class are readily identifiable through Defendant's records.

67. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least one million people. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

68. **Commonality and Predominance.** This action involves common questions of law and fact to Plaintiff's minor child and the Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant owed Plaintiff's minor child and the other Class members a duty to adequately protect their PII;

b. Whether Defendant owed Plaintiff's minor child and the other Class members a duty to implement reasonable data security measures due to the foreseeability of a data breach;

c. Whether Defendant owed Plaintiff's minor child and the other Class members a duty to implement reasonable data security measures because Defendant accepted, stored, and maintained highly sensitive information concerning Plaintiff's minor child and the Class;

d. Whether Defendant knew or should have known of the risk of a data breach;

e. Whether Defendant breached its duty to protect the PII of Plaintiff's minor child and other Class members;

f. Whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's minor child's and the Class's PII from unauthorized theft, release, and disclosure;

h. Whether proper data security measures, policies, procedures and protocols were in enacted within Defendant's offices and computer systems to safeguard and protect Plaintiff's minor child's and the Class's PII from unauthorized theft, release or disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiff's minor child's and the Class's injuries;

j. Whether Plaintiff's minor child and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiff's minor child and the Class are entitled to recover damages; and

l. Whether Plaintiff's minor child and the Class are entitled to other appropriate remedies including injunctive relief.

69. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of her minor child and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

70. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's minor child's PII, like that of every other Class member, was misused and improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

71. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interest of the members of the Class, and has retained counsel experienced in complex consumer class action litigation and intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

72. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
Negligence
(on behalf of Plaintiff and the Class)

73. Plaintiff realleges and incorporates Paragraphs 1 through 72 above as though fully stated herein.

74. Defendant collected, maintained, and stored Plaintiff's minor child's and the Class's PII for the purpose of facilitating medical treatment to Plaintiff's minor child and the Class.

75. Plaintiff's minor child and the Class are a well-defined, foreseeable, and probable group of individuals that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of

Defendant's business requires patients to disclose PII to receive adequate care, including, but not limited to, medical histories, dates of birth, social security numbers, addresses, phone numbers, and medical insurance information. That information is then exchanged with Defendant by N.L.'s and the Class's medical providers as part of the services that Defendant provides to its customers. Therefore, Defendant uses, handles, gathers, and stores the PII of N.L. and the Class and, additionally, solicits and stores records containing N.L.'s and the Class's PII.

76. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that its repository of a host of PII for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard the PII by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff's minor child and the Class of inadequate data security created a duty to act reasonably and safeguard the PII.

77. Defendant owed a duty to Plaintiff's minor child and the Class to exercise reasonable care in safeguarding and protecting their PII in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

78. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's minor child's and the Class's PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

79. Defendant also had a duty to timely disclose to Plaintiff and her minor child and the Class that their PII had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiff and her minor child and the Class may take appropriate measures to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

80. Defendant also should have known that, given the PII it held, Plaintiff's minor child and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiff's minor child's and the Class's PII had security vulnerabilities susceptible to cyber-attacks.

81. Despite that knowledge, Defendant implemented unreasonable data security measures that allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of

time, and access or steal a host of personal and healthcare information on thousands of Defendant's customers' patients.

82. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

83. Defendant breached its duty to N.L. and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their PII, allowing unauthorized access to N.L.'s and the Class's PII, and failing to recognize the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's minor child's and the Class's PII.

84. But for Defendant's wrongful and negligent breach of its duties, N.L.'s and the Class's PII would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

85. Additionally, Defendant failed to reasonably notify Plaintiff and her minor child and the Class of the Data Breach. Defendant waited over four weeks after discovering the Data Breach — including two weeks while the third party still had access to Defendant's systems after Defendant was aware of suspicious activity — to inform Plaintiff and her minor child and the Class that their information was accessed. The unreasonable delay in notifying Plaintiff and the Class of the breach

robbed them of the opportunity to take measures to protect against the misuse of their information and to monitor their accounts.

86. As a result of Defendant's negligence, Plaintiff's minor child and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

COUNT II
Negligence *Per Se*
(on behalf of Plaintiff and the Class)

87. Plaintiff realleges and incorporates Paragraphs 1 through 72 above as though fully stated herein.

88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

89. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's minor child's and the Class's PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

90. To provide its health records and management services, Defendant collected, maintained, and stored Plaintiff's minor child's and the Class's PII.

91. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

92. Plaintiff's minor child and the Class are within the group of individuals the FTC Act was designed to protect and the harm to these individuals is a result of the Data Breach. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff's minor child and the proposed Class.

93. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff's minor child and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

94. As a direct and proximate result of Defendant's negligence, Plaintiff's minor child and the Class have been injured as described herein and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

95. WHEREFORE, Plaintiff respectfully prays for judgment in their favor as follows:

a. Certification the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel, Zimmerman Reed LLP, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

96. Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: May 22, 2023

/s/ MaryBeth Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Facsimile: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Brian C. Gudmundson*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Counsel for Plaintiff and the Proposed Class

* To be admitted *pro hac vice*

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: May 22, 2023.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON